THE CYBER DEFENSE REVIEW
In press, 9 pages
https://doi.org/10.55682/cdr/wkpx-twrz

SENIOR LEADER PERSPECTIVE

Defeating the Cyber Invasion with a National Cyber Force

Franklin D. Kramer[1], Robert J. Butler*[2], Melanie Teplinsky[3]

[1]Atlantic Council, Washington, DC, USA
[2]Cyber Strategies LLC, College Station, TX, USA
[3]American University Washington College of Law, Washington, DC, USA

The revelation of China-sponsored Typhoon cyberattacks against critical infrastructure signals an escalation of threat facing the United States. The scope of adversarial penetration and nature of these attacks—including malware inserted into thousands of computers—constitutes nothing less than a cyber invasion. Currently, the United States Government (USG) lacks unity of effort and comprehensive resources to deter and defeat such determined adversaries. Countering this cyber invasion requires a transformed national cyber force model, one that seamlessly integrates capabilities and expertise from America's civilian cyber workforce. To achieve this, the authors recommend five specific actions: 1) establish an Integrated Cyber Provider Corps (ICPC) of cybersecurity and cloud service providers under the National Cyber Director (NCD) to scale active cyber defense for critical infrastructure; 2) create a national lab cyber cohort of experts from research centers and national laboratories to provide technical direction and support for cyber defense and offensive planning; 3) expand cyber capabilities of the National Reserve Force and utilize them more frequently to bridge federal and state coordination gaps; 4) establish a civilian cyber reserve force to leverage private sector expertise and resources to increase domestic cybersecurity capacity; and 5) develop regional resilience districts comprised of private critical infrastructure owners and operators, and their federal, state, and local government agency partners, to ensure continuity and build resilience of critical national defense and commerce hubs.

Keywords: national cyber director, cybersecurity, critical infrastructure, resilience, national security

* Corresponding author: bbutler@cyberstrategies.org

Franklin D. Kramer is a distinguished fellow and board director at the Atlantic Council. Kramer has served as a senior political appointee in two administrations, including as assistant secretary of defense for international security affairs. At the U.S. Department of Defense, Kramer was in charge of the formulation and implementation of international defense and political-military policy, with worldwide responsibilities including NATO and Europe, the Middle East, Asia, Africa, and Latin America. In the nonprofit world, Kramer has been a senior fellow at CNA; chairman of the board of the World Affairs Council of Washington, DC; a distinguished research fellow at the Center for Technology and National Security Policy at National Defense University; and an adjunct professor at the Elliott School of International Affairs at George Washington University. Kramer's areas of focus include defense, both conventional and hybrid; China, including managing competition, military power, and China-Taiwan-U.S. relations; NATO and Russia; cyber, including resilience and international issues; trade and globalization; irregular conflict and counterinsurgency; innovation and national security.

Robert (Bob) J. Butler serves as the Managing Director for Cyber Strategies LLC, a full-service cyber security and risk management firm. In this role, he has functioned as a consultant, board member and senior advisor for both public and private sector clients. Bob retired from the Air Force after 26 years of active duty service in the intelligence, information technology and cybersecurity communities, culminating his military career serving as the first commander of NSA's Texas Cryptologic Center. After his military service, Bob served twice as a Defense Senior Executive to include posting as the first Deputy Assistant Secretary of Defense for Cyber and Space Policy. Bob has also served as a Senior Vice President at AECOM where he functioned as the chief of operations for a global corporate critical infrastructure protection campaign, and as Chief Security Officer for IO Data Centers where he oversaw the development and implementation of all security activities for a multi-million dollar data center services and product company with locations in the U.S., UK and Singapore.

Melanie J. Teplinsky is a cyber law and policy expert with experience spanning private sector, government, and academia. She is an adjunct professor and senior fellow in the Technology, Law, and Security Program at American University, Washington College of Law. Ms. Teplinsky began her career at the National Security Agency, subsequently serving in NIST's Computer Security Lab and OMB's OIRA. She practiced technology law at Steptoe & Johnson LLP before serving (pre-IPO) on the advisory board for CrowdStrike, Inc. She writes and speaks on a wide array of issues including software liability, ransomware and cryptocurrency, data protection, and cyber espionage. Notable engagements include serving as an expert panelist at the White House Legal Symposium on Software Liability (2024); briefing NIST's Information Security and Privacy Advisory Board on software liability issues; and exploring the private sector's role in conflict as part of a Congressional Cybersecurity Caucus-hosted Hill briefing. Recent publications include "Shields Up For Software" (co-authored with Derek Bambauer) and several cybersecurity pieces co- authored with Franklin D. Kramer and Robert J. Butler).

UNDERSTANDING THE PROBLEM AND OPPORTUNITY

The disruption caused by China's sophisticated "Typhoon" campaigns confirms a new level of malicious threat and the need to bolster homeland defenses in the United States (McCrary Institute for Cyber and Critical Infrastructure Security 2025). These incursions go beyond standard espionage; the depth of penetration and installation of malware across thousands of systems represents a functional cyber invasion into the United States. The Salt Typhoon infiltration of telecommunications infrastructure by the Chinese Communist Party (CCP) exposed pervasive vulnerabilities in U.S. national security, economic, and public safety postures (U.S. Congress 2025). Similarly, the Volt Typhoon attack revealed deep CCP penetration into the energy sector and other critical infrastructure assets foundational to both national security and societal well-being at large (Microsoft Threat Intelligence 2023). Russian and Iranian nation-state actors, among others, have demonstrated similar capabilities and intent (NSA, CISA, and FBI 2024; CISA 2024). A clear pattern emerges: adversaries are running continuous offensive cyber campaigns targeting the U.S. homeland and the critical services American citizens rely on most.

The advent of a new U.S. administration and rapidly evolving technologies—such as generative artificial intelligence (AI) and quantum computing—offer a pivotal opportunity to address these escalating digital threats in new and more effective ways. However, successfully changing course requires resolving a fundamental structural asymmetry. Unlike autocratic regimes that utilize state-owned enterprises to pursue national interests through whole-of-nation activity, ***the United States Government (USG) currently lacks the unity of effort and comprehensive resourcing to defeat and deter cyber exploitation and attack—or potential invasion—by determined adversaries.***

REMEDIES: PAST AND FUTURE

Fifteen years ago, recognizing that cyberspace had emerged as a new domain of warfare, the U.S. stood up Cyber Command (USCYBERCOM) to help defend the nation (DoD 2011). The USCYBERCOM force generation model currently consists of active duty and reserve forces from all military services and the U.S. Coast Guard (USCG). Crucially, USCYBERCOM leverages the significant intelligence resources of the National Security Agency (NSA) through collocation at Fort Meade and a dual-hat command structure. The Command has three main focus areas: defending the Department of War Information Network (DoWIN, formerly DoDIN), supporting combatant commanders in executing global missions, and strengthening the nation's ability to withstand and respond to cyber attack.[1]

The creation of USCYBERCOM was an essential step toward standing up a military force to defend against and respond to cyber threats. However, it has proven insufficient on its

1. https://www.cybercom.mil/About/Mission-and-Vision/

own to generate the capabilities and expertise needed at scale for comprehensive national cybersecurity. Consequently, civilian agencies have evolved to fortify facets of the nation's non-military cyber defenses. The Cybersecurity and Infrastructure Security Agency (CISA) anchors this effort by taking a collaborative support approach towards critical infrastructure security and resilience—enabling cyber threat intelligence sharing, issuing joint advisories, and providing guidance to state, local, and industry partners.[2] Working in tandem, the Federal Bureau of Investigation (FBI) leads investigations into cyber intrusions and crimes,[3] while the Department of the Treasury enforces sanctions to disrupt the financial networks of malicious cyber actors and promotes the cyber resiliency of financial systems and institutions (U.S. Department of the Treasury 2024, 17–22). Nevertheless, the U.S. continues to face increased malicious cyber activity by criminals and sophisticated nation-states determined to harm national and public interests.

Experts have increasingly raised concerns about the inadequacy of the current national cyber model. Notably, the Congressionally-sponsored Cyberspace Solarium Commission (2020) Report called on national leaders to take more aggressive steps to secure cyberspace (Atlantic Council 2023; Miller and Butler 2022). Most of these calls to action highlight the necessity of a better-coordinated, well-resourced whole-of-nation approach that continuously plans and sustainably enables both active defensive and offensive actions. These reports suggest the need for a much larger cyber workforce and emphasize a critical gap: the current model fails to sufficiently leverage the private sector, which operates the vast majority of U.S. critical infrastructure. ***Defeating a cyber invasion requires a fundamentally different cyber force model–one that fully integrates the capabilities and expertise of America's civilian cyber workforce and operates seamlessly across the public-private sectors and civil-military seam.***

BUILDING A NATIONAL CYBER FORCE

With the creation of the Office of the National Cyber Director (NCD) at the White House in 2021, the U.S. now has a recognized leader for coordinating a whole-of-nation effort in cyberspace (Office of the National Cyber Director, n.d.). While currently constrained by limited resources, the USG has proven mechanisms for marshalling public sector expertise into cohesive capability packages. Accordingly, we recommend the following:

- **Establish an Integrated Cyber Provider Corps (ICPC or Corps).** Comprised of high-end industry cybersecurity and cloud service providers, this Corps will collaborate to scale active cyber defense for critical infrastructure through rapid innovation, investment, and the adoption of proven methods.

2. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience
3. https://www.fbi.gov/investigate/cyber

- **Form a national cyber lab cohort to build technical expertise.** Drawing from Federally Funded Research and Development Centers (FFRDCs), University Affiliated Research Centers (UARCs), and national laboratories, this body of technical experts and established research and development (R&D) capabilities will provide technical direction to the NCD and policy-makers. Their focus will be on defensive and offensive planning to counter and deter nation-state adversaries.
- **Increase utilization and capacity of the National Reserve Force.** By employing National Guard and Reserve cyber forces at greater frequency, the USG can bridge coordination gaps between federal, state, and industry partners.
- **Augment domestic cybersecurity with a civilian cyber reserve force.** By formalizing a non-military service pathway for cyber professionals, the USG can harness the nation's distributed cyber workforce and private sector talent, expertise, and resources. The force would significantly increase the depth of technical cyber resources available for the nation.
- **Develop regional resilience districts.** These districts will unite critical infrastructure owners with federal, state, and local agencies. Their mission is to ensure the continuity and resilience of key defense and national commerce hubs.

An Integrated Cybersecurity Provider Corps

To begin such an effort, a consortium of cybersecurity and cloud service companies should be established to focus on providing effective cybersecurity for the critical infrastructure most relevant to military activities, continuity of government, and the economy (Atlantic Council 2023). Broadly speaking, this Corps should be able to provide high-end cybersecurity and secure cloud services ranging from helping the most critical entities create and sustain zero trust architectures (ZTA) (NIST 2020) to deploying defensive threat hunting capabilities and generating and executing active defenses. Some of these services are already being undertaken on key systems through contractual arrangements with private firms, but it is imperative that *all* key systems receive such services.

The companies that form the Corps will also have the collective expertise to rapidly leverage emerging technologies, such as ephemeral authentication and agentic AI, as essential elements for creating and growing ZTAs in the face of a rapidly changing threat landscape. Importantly, this Corps could leverage commercial relationships and maintain close relationships with owners and operators of critical infrastructure. The Department of Homeland Security (2018) Section 9 list of companies "where a cybersecurity incident could reasonably result in catastrophic regional or national effects" could provide the basis – or, at a minimum, a starting point – for identifying the infrastructures most critical in wartime (CISA 2021).

A National Cyber Lab Cohort

As was the case in the aftermath of World War II, FFRDCs, UARCs, and national laboratories are uniquely qualified to help guide the nation in developing and using new technologies and concepts for national security. The U.S. has a rich tapestry of government-supported and affiliated academic research and development institutions with deep knowledge and experience across the cyberspace domain and critical infrastructure sectors. Most, if not all, of these institutions already have individual cyber programs underway. Leveraging these existing structures harnesses this expertise by creating a pathway for that knowledge to inform broader cybersecurity design, planning, and implementation. Formation of a National Cyber Lab Cohort would facilitate unity of effort, enabling top technical experts to work together in a coordinated fashion to bring their deep technical expertise to bear on our nation's most pressing cybersecurity problems.

Based on its technical and operational expertise in both government and critical infrastructure, a National Cyber Lab Cohort consisting of cyber experts from the FFRDCs, UARCs, and national labs, under the direction of the NCD, would be ideally suited to pioneer solutions in developing and providing national red teams and high-end reverse engineering support across government and industry critical infrastructure.

An Expanded National Military Reserve Force

The National Reserve Force includes both a federal reserve corps and a National Guard that can support both federal and state needs. Congress has recognized the National Guard's contributions to cybersecurity and has directed the Pentagon to evaluate expanding Guard cyber missions (CISA 2021). As citizen-soldiers, the National Guard provides critical cyber expertise and synchronization of effort at the federal, state, and regional levels.

As part of this effort and to meet the needs across state lines, the NCD would work with National Guard leaders and state government leadership to develop cross-state agreements and enable greater unity of effort in cyber defense across the homeland. Generating regional capabilities will help ensure that a critical mass of highly capable cybersecurity professionals will have had the opportunity to train and exercise together prior to a contingency in which their talents are needed. Lessons learned from Guard involvement in the State Partnership Program[4] can usefully be applied to the Guard's defensive role and shared from one Guard unit to another. In addition to these defensive mission activities, the National Guard can play a critical role in augmenting the cadre and expertise of U.S. military offensive cyber operators.

Another significant element to scaling an overall National Reserve Force and bolstering private sector expertise for national cybersecurity campaign planning can be found in the

4. See https://www.nationalguard.mil/Leadership/Joint-Staff/J-5/International-Affairs-Division/State-Partnership-Program/

recent U.S. Army initiative to create an Executive Innovation Corps by bringing senior executives from firms such as Meta, Palantir, and OpenAI into the Reserves (Harper 2025). This initiative should be expanded to all services and function as a group of senior advisors to the NCD and other national cybersecurity leaders.

A Civilian Cyber Reserve Force

The nation would benefit greatly – in both scaling capacity and capability – by expanding opportunities for civilian cyber service. Multiple states, including Michigan, California, Maryland, Ohio, and Texas, are already experimenting with volunteer programs, and others are considering the same. The National Defense Authorization Act (NDAA) for 2024 authorized the Secretary of the Army to conduct a pilot program to establish a civilian cybersecurity reserve to provide USCYBERCOM with additional talent and human resources (Brumfield 2024). Operating as a non-combatant entity outside military command, the civilian cyber reserves would flexibly support state, local, and critical infrastructure partners (e.g., water/wastewater utilities) that lack adequate resources. While states would tailor structures to available assets and unique security needs, the NCD would centrally coordinate the distributed capabilities across state lines and regional resilience districts. The service would leverage private sector innovations—supported by the ICPC and national lab cohort—to integrate essential operational functions, including intelligence sharing, workforce management, and assurance.[5]

Civilian cyber reserves could be further expanded through volunteer commitments of cybersecurity experts from corporate America. Under this construct, companies would provide paid time off to employees who volunteer and commit time to serve in the civilian cyber reserves. Several high-tech companies and professional services organizations already offer benefits like this to their employees. In line with opportunities in the legal profession, companies with competent, well-paid cyber professionals could be incentivized to encourage their employees to perform "pro bono" cybersecurity work.[6]

5. Existing whole-of-sector collaborations, such as the Department of the Treasury's Project Fortress 2025, offer proven models for automated threat feeds and cross-sector professional collaboration. See https://home.treasury.gov/system/files/216/Project-Fortress-Brochure.pdf

6. The American Bar Association's Pro Bono Initiative Challenge offers some useful lessons for setting up such a program. The initiative spurred large law firms to provide institutional support for their attorneys to provide pro bono legal services. See https://www.probonoinst.org/wp-content/uploads/2024_PBI_Challenge-ReportFinal.pdf

Individual participation in the proposed civilian cyber reserve could also be incentivized through a combination of the same benefits used to attract and retain volunteer firefighters, namely, compensation (including paid time off as proposed above), tax benefits,[7] and retirement programs.[8]

Regional Resilience Districts

At the local level, a regional resilience district is a sustained engagement among public and private entities around critical commerce and defense hubs. It is designed to mitigate and, if required, respond to high-consequence security risks through effective collaboration among private, state, local, and federal entities. Examples of such hubs would include national ports of significant commercial import or military installations. Along these lines, there are compelling arguments for "operationalizing military installations as coordination nodes, or 'seeds,' for regional cyber resilience" (Lee 2025). Importantly, these regional resilience districts require both industry and government champions and the necessary authorities and resources to incentivize sustained risk mitigation.[9]

The risks to be considered for mitigation and response by regional resilience districts will include both natural and manmade threats, as well as the potential conjunction of both. The geopolitical context to be planned for will include heightened contestation with nation-state adversaries (especially Russia, China, Iran, and North Korea), non-state actors (criminals and terrorists), and severe weather/climate effects (hurricanes, flooding, heat, water shortage). In this context, regional preparation for the possibility of an armed attack—kinetic or non-kinetic—will be explicit and deliberate. In the case of cyber risk mitigation, the leadership of these regional resilience districts will work closely with the NCD and the national cyber leadership team.

CONCLUSION

The new Administration and national leadership stand at a crossroads in how we use and protect cyberspace. A whole-of-nation approach to cybersecurity with a synchronized national and regional force model that effectively leverages the unparalleled U.S. cyber talent pool is foundational to a safer and more prosperous America. Failure to adopt such an approach

7. Pursuant to the Volunteer Responder Incentive Protection Act (VRIPA), the first $600 of volunteer firefighter stipends (and other incentives) are exempt from federal tax. See https://www.volunteerfirefighter.org/benefits. Section 103 of the Taxpayer Certainty and Disaster Relief Act of 2020 makes this federal tax exemption permanent. See https://www.nvfc.org/federal-tax-exemption-for-volunteer-responders-made-permanent/.

8. Some volunteer fire departments provide pension and retirement benefits as an incentive for long-term service. See https://volunteerguide.org/2024/09/06/do-volunteer-firefighters-get-paid/. "Colorado has a state match program that helps local governments provide retirement benefits to attract volunteers. Eligible entities must contribute funds generated from taxes, which the state then matches based on a statutory calculation." See https://dlg.colorado.gov/volunteer-firefighter-pension-fund.

9. The Houston Ship Channel Security District, for example, is a sustained partnership between the USCG Captain of the Port, industry partners, and other government entities. See https://hscsd.org/.

will only further embolden our adversaries to continue their cyber campaigns and attacks against the U.S.

REFERENCES

Atlantic Council. 2023. *The Sixth Domain: The Role of the Private Sector in Warfare.* Technical report. Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2023/10/The-sixth-domain-The-role-of-the-private-sector-in-warfare-Oct16.pdf.

Brumfield, Cynthia. 2024. "Civilian Cyber Reserves Gaining Steam at the US Federal and State Levels." *CSO Online* (January 24, 2024). https://www.csoonline.com/article/1297690/civilian-cyber-reserves-gaining-steam-at-the-us-federal-and-state-levels.html.

CISA (Cybersecurity and Infrastructure Security Agency). 2021. *Support to Critical Infrastructure at Greatest Risk.* https://www.cisa.gov/resources-tools/resources/support-critical-infrastructure-greatest-risk-section-9-report-summary.

CISA (Cybersecurity and Infrastructure Security Agency). 2024. *Iran: Advanced Persistent Threats.* Accessed December 9, 2025. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran.

Cyberspace Solarium Commission. 2020. *CSC 2.0 Report.* Technical report. Accessed December 9, 2025. https://www.solarium.gov/report.

Department of Homeland Security. 2018. *EO 13800 Section 9 Report Summary.* https://www.cisa.gov/sites/default/files/publications/EO-13800-Section-9-Report-Summary-20180508-508.pdf.

DoD (Department of Defense). 2011. *Department of Defense Strategy for Operating in Cyberspace.* Technical report. Accessed December 9, 2025. https://csrc.nist.gov/csrc/media/projects/ispab/documents/dod-strategy-for-operating-in-cyberspace.pdf.

Harper, Jon. 2025. "Army Recruits Officers from Meta, OpenAI and Palantir to Serve in New Detachment." *DefenseScoop* (June 13, 2025). https://defensescoop.com/2025/06/13/army-detachment-201-executive-innovation-corps-meta-openai-palantir/.

Lee, Michaela. 2025. "Beyond the Fence Line: Operationalizing Civil-Military Cyber Coordination at U.S. Military Installations." *The Cyber Defense Review* 10 (2). https://doi.org/10.55682/cdr/s1yk-adc9.

McCrary Institute for Cyber and Critical Infrastructure Security. 2025. *Code Red: A Guide to Understanding China's Sophisticated Typhoon Cyber Campaigns.* Technical report. Auburn University. Accessed December 9, 2025. https://mccraryinstitute.com/app/uploads/2025/10/McCrary-Institue-Code-Red-Release-Ready.pdf.

Microsoft Threat Intelligence. 2023. *Volt Typhoon Targets US Critical Infrastructure with Living-off-the-Land Techniques,* May. Accessed December 9, 2025. https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.

Miller, James N., and Robert J. Butler. 2022. *National Cyber Defense Center.* Technical report. Johns Hopkins University Applied Physics Laboratory. Accessed December 9, 2025. https://www.jhuapl.edu/sites/default/files/2022-12/NationalCyberDefenseCenter.pdf.

NIST (Standards, National Institute of, and Technology). 2020. *Zero Trust Architecture.* NIST Special Publication 800-207. https://www.nist.gov/publications/zero-trust-architecture.

NSA, CISA, and FBI (National Security Agency, Cybersecurity and Infrastructure Security Agency, and Federal Bureau of Investigation). 2024. *Russian Military Cyber Actors Target US and Global Critical Infrastructure.* Technical report. September. https://media.defense.gov/2024/Sep/05/2003537870/-1/-1/0/CSA-Russian-Military-Cyber-Target-US-Global-CI.PDF.

Office of the National Cyber Director. n.d. *Office of the National Cyber Director.* Accessed December 9, 2025. https://www.whitehouse.gov/oncd/.

U.S. Congress. 2025. *Hearing Transcript: HHRG-119-GO06.* Committee on Oversight and Accountability. Accessed December 9, 2025. https://www.congress.gov/119/meeting/house/118084/documents/HHRG-119-GO06-Transcript-20250402.pdf.

U.S. Department of the Treasury. 2024. *Treasury Strategic Plan 2022–2026: 2024 Print Update.* Technical report. Washington, D.C. https://home.treasury.gov/system/files/136/TreasuryStrategicPlan-FY2022-2026-2024-print-update.pdf.